Veritas
Stalking Advocacy Service

CYBER SAFETY ADVICE

Sections include:

- Secure your Apps
- Secure your email account
- Privacy on the web

Secure your Apps:

WhatsApp

WhatsApp is possibly the most popular messaging app around, in order to maintain some privacy, you may want to change your last seen privacy settings in WhatsApp. Here’s how you do it:

Google Android

1. Launch **WhatsApp** from your Home screen or the app drawer
2. Tap on the **More options** button (it looks like three dots aligned vertically and is in the top right-hand corner of your screen)
3. Tap on **Settings**
4. Tap on **Account**
5. Tap on **Privacy**
6. Tap on **Last seen**
7. Tap on the option you desire

Apple iOS

1. Launch **WhatsApp** from your Home screen
2. Tap on the **Settings** tab (it's the gear icon in the bottom right corner of your screen)
3. Tap on the **Account** button (it's the blue box with the white key in the middle)
4. Tap on the **Privacy** button
5. Tap on the **Status** button (This will show you a menu with three options)
6. Tap on the option you desire

Options

Everyone: All WhatsApp users get Last seen updates about you.
My contacts: Only people on your contacts list get Last seen updates.
Nobody: Other WhatsApp users will no longer get any Last seen updates about you.

Messenger

The appeal of Messenger is that it is attached to Facebook and so can be linked to a user's friends even if they aren't in their phone contacts. It can be used for voice and video calling but, unlike WhatsApp, it currently doesn't use end-to-end encryption unless the conversation is marked as 'secret'. Secret conversations are encrypted end-to-end, but all others currently aren't.
To access the security setting in Messenger for both Google Android and Apple iOS, follow the steps below:

1. Login to **Facebook Messenger**
2. Check the **top right corner** of Facebook Messenger
3. Tap your **profile picture**
4. Scroll down until you get to **Account Settings**
5. Tap **Account Settings**
6. You now have access to Security within Account Settings

Facebook

Secure your Facebook account:

1. Login to **Facebook**
2. Check the **bottom right corner** of Facebook
3. Scroll down until you get to **Settings**

Account Settings:

- Select the username that other users will see.
- Assign an email address – it is recommended that you do not use your work email

Security:

- Nominate 3-5 friends to contact if you get locked out of your account
- See all active Facebook sessions where your account is logged in and you can log any sessions out. If you see anything suspicious leave logged in and report to the Police.
- Get login alerts
- Add Two-factor authentication

Privacy:

- Make sure only your 'Friends" can see what you have posted. It is recommended you have your Friend list privacy to 'Only me.'
- Change Face recognition to No
- Profile and tagging: Make sure that only you can add posts or approve posts friends tag you in. Review and manage tags posted by others that mention you.
- Location: View your location history and delete information if needed.

House Party

Houseparty has millions of downloads during the coronavirus pandemic, and it has become a very popular video socialising app. However, from a privacy perspective, there's one obvious issue that you may want to take note of before organising games and parties: they are open to any of your friends and friends of friends unless you lock the "room" where you're playing.

Here's how you can secure that feature:

Google Android

To lock all rooms that you enter by default:

1. Tap on **Account**
2. Tap on **Settings**
3. Tap the **Private Mode** toggle to on

Apple iOS

1. Once in a chat, tap the three vertical dots at the bottom left of the screen
2. Tap the **padlock** to Lock the Room

LinkedIn

To secure your LinkedIn:

1. Tap on **Account**
2. Tap on **Settings** and scroll to:

Login and Security

- You can edit your email address- it is recommended that you do not use your work email.
- Avoid using your phone number
- You can see all the places your account is signed in and see details of individual sessions and log them out. If you see anything suspicious leave logged in and report to the Police.

Site Preferences:

- You can restrict who can see your profile picture by selecting 'Your Connections'

3. Tap on **Privacy**

- You can edit your public profile and how it is viewed. Choose the 'Nobody' option to manage who can discover your profile from your email address and phone number.

Twitter

To secure your Twitter:

1. Login to **Twitter**
2. Tap on the three horizontal lines in the **top left corner** of Twitter
3. Tap on **Settings and Privacy**
4. You now have access to Security within Account Settings

Unless your account is private, once you Tweet, anyone around the world with access to Twitter can see it. You can protect your tweets by tapping on the Privacy and safety section.

In Privacy and Safety, you can:

- Change your Direct Messaging settings to not allow anyone to message you
- Unsure read receipts so anyone messaging you cannot see if you have read their message
- Change how people discover you we would recommend you do not allow people to discover you via your email or phone number.
- Mute accounts
- Disable precise location settings

Instagram

To secure your Instagram:

1. Login to **Instagram**
2. Tap on the profile icon in the **bottom right**
3. Tap on the three horizontal lines in the **top right corner**
4. Tap on **Settings**
5. You now have access to Security within Account Settings

Privacy:

- You can make your profile private which means only your followers will see your posts. If you were not private previously anyone who is following you will still see your posts. You can manually go through your followers and remove them. Any new followers will have to request approval by the account owner before they can follow the account.
- You can block new comments from people they will still be able to see their comments however no one else will.
- You can change who can Tag you in photos.
- You can hide your story from followers and control who can reply.

Security:

- You can view where your account is logged in
- Add Two-factor authentication

Account:

- You can switch off Contact syncing to avoid synchronising and storing your contacts on the server.

Snapchat

To secure your Snapchat:

1. Login to your account and go to **Settings**
2. Scroll to Two-Factor Authentication and add this
3. Scroll to Manage and adjust privacy settings accordingly. We suggest that you only allow 'My Friends' to view your story and contact you.
4. While in the manage section click on option in the **Additional services** section and then click on '**Permissions**'. We suggest that you do not allow Snapchat to use your location this means Snapmaps will not be in use.

TikTok

To secure your TikTok:

1. Login to your account and go to **Settings**
2. Click on **Manage My Account**, this will show you any security alerts in the past 7 days and when your account is logged in.
3. Click out of this section and click on **Privacy and Security**, switch on **Private Account** mode to make your account more secure. Scroll down and select your safety settings such as who can comment on your videos, we suggest you select **Friends.**

Zoom

Zoom has emerged as a very popular tool for online meetings, training and other communication activities during the coronavirus pandemic of 2020, but there are risks associated with any app:

•**Phishing ploys**: messages inviting participants to click on *malicious links* to fake meetings, or uninvited guests sharing malicious links during a meeting.
•**Privacy risks**: users including *sensitive information* in their Zoom profiles, which can be viewed by meeting participants.
•**Live recording**: hosts allowing participants to *record the session*, or participants using mobile phones to record it surreptitiously.
•**'Zoom bombing'**: unauthorised participants *hijacking meetings*, often because password access was not setup or meeting passwords were shared insecurely.

Amazon

Secure your Amazon:

- Amazon lists are visible to the public by default. In order to make your purchases more private you need to manage your lists. You can delete them by clicking on ‘**Manage list**’ and then clicking ‘**delete**’. Alternatively, in the ‘**Manage list**’ option you can change your list from public to private.
- It is not recommended that you link your social media accounts with your Amazon profile.

Secure your Email Account

There are many different email vendors on the web, but they all offer many features to secure your account. In a situation where email accounts have previously been shared, it is a good idea to create a new account to ensure that an ex-partner no longer has access to your emails.

An email account is where we hold all of our important business: shopping confirmations, banking messages and, most importantly, password reset requests. With unauthorised access to an email account, a password can be reset for almost all other accounts.

Two ways in which you can greatly reduce the risk of your email account being compromised are having a strong password and using two factor authentications. Here’s how to do these:

To create a strong password:
This needs to be memorable but also strong. To do this, come up with your own formula to replace some of the letters with numbers.

Here is an example of letters that are replaced by numbers based on their similarity:

A	= 4
E	= 3
I	= 1
O	= 0
S	= 5
Z	= 2

Think of a place and date that has meaning to you: **Amsterdam 26th March 1996**

In order to create that memory into a secure password, just take it through two simple stages:

Remove all the spaces and convert the date:	**Amsterdam260396**
Apply the above formula:	**Am5t3rd4m260396**

If you wish to add an extra layer of security to your password, or if it is required of the site that you are setting an account up for, you can add in a symbol too: **$Am5t3rd4m260396**

App stores also offer password generator apps, should you wish to create random, strong passwords. However, you will need a way of remembering these once generated!

Two Factor Authentication (2FA)

This is an extra layer of security which guarantees a more secure account for you online.
Many apps and websites have 2FA built in as an option, but you have to find it in the settings.

Except for online banking, it is rarely switched on as a default, but it is extremely important to use this feature wherever it is offered.

Some banks use card readers or PIN pads to allow account holders to log in to their accounts, others text or phone a code to their registered device. With other services, such as email accounts or subscriptions, you may be given the option to either receive a text code or use an authentication app.

These apps are available to download for free from the app stores, and the most popular are **Google Authenticator** and **Microsoft Authenticator**. However, there are many others, and you may be asked to use a particular one.

What to do before setting up a 2FA?

- Google Authenticator has been downloaded from the Google Play Store (Google Android) or the App Store (Apple iOS)
- A barcode or QR scanner is installed on your phone. If one isn't, Google Authenticator will ask you to do so.
- You have a Google account set up (other authenticator apps do not require this).
- You have visited the site or app that is requesting the 2FA setup.

Example: Setting up 2FA on Facebook

1. On your phone, open the **Facebook** app
2. Tap the 3 horizontal bars at the **bottom right** of the screen
3. Scroll down and tap **Settings**
4. Scroll down and tap **Security** and login
5. Scroll down to Two-factor authentication and tap **Use two-factor authentication**
6. Scroll down to **Select a security method** and tap **Authentication app**
7. You'll see the following pages with a QR code at the top and some instructions below
8. To set up the 2FA on a different device, **scan the QR code** with a QR scanner
9. To set up the 2FA on the same device that the Facebook account is logged in to, tap set up on same device. You should be prompted to open the Google Authenticator app.

10. If you are offered a different installed authentication app, you can use that one and follow the instructions or enter the code into Google Authenticator manually:

- Tap and hold the **long code** under or **enter this code** into your authentication app
- Once the code has been copied (a popup will tell you), open the Google Authenticator app
- In the Google Authenticator app, **tap the plus symbol** at the top right of the screen and select **Manual entry**
- Enter the details for the Account (e.g. Facebook username)
- Paste the details of the code copied in the first stage above into the Key
- Keep the Time-based toggle switched to **On** (it is by default)
- Return to the Facebook app where you will be asked to enter the current 6-digit code for Facebook showing in the Google Authenticator app
- You will then be asked to re-enter your Facebook login password to complete the 2FA setup

You will now be able to use the Google Authenticator app whenever Facebook senses a login.

Privacy on the Web

MICROSOFT EDGE / GOOGLE CHROME / FIREFOX / SAFARI

There are a number of different web browsers that can be used to access the information on the worldwide web, but the most commonly used are Microsoft's Edge (formerly Internet Explorer), Google Chrome, Mozilla Firefox and Apple's Safari.

Your web browsing history holds valuable information, not only for the commercial businesses that thrive on targeted sales but also for anyone who has unauthorised access to an account linked to your web browser.

For example, if you are logged in to a Google account and search the web using Google search, then your history will be stored at Google by default until you make changes (it can be disabled on your account). If someone has access to your Google account (or, indeed, your device), they will also be able to see exactly what you have been looking at on the web, and this can be useful information for them in certain circumstances.

The easiest way to avoid this is to search the web in a private browsing mode. This will allow you to browse the web without your browser saving any browsing history, cookies and passwords. However, your browsing will still be visible to your Internet Service Provider and your employer, should you be using a work device.

Here's how you can browse privately:

Microsoft Edge

Windows

1. Open **Microsoft Edge**
2. Click on the 3 horizontal dots in the top right of the window
3. Click on **New InPrivate window**
4. Start browsing privately

Android / iOS

1. Open **Microsoft Edge**
2. Tap on the 3 horizontal dots in the bottom right of the screen
3. Tap on **New InPrivate** tab
4. Start browsing privately

Google Chrome

Windows / Mac OS

1. Open **Google Chrome**
2. Click on the 3 vertical dots in the top right of the window
3. Click on **New incognito window**
4. Start browsing privately

Tip - Keyboard shortcuts to open an incognito window: Ctrl-Shift-N (Windows) or Command/cmd-Shift-N (Mac)

Android / iOS

1. Open **Google Chrome**
2. Tap on the **tabs** icon in the top right of the screen
3. Tap on the 3 vertical dots in the top right of the screen
4. Tap on **New Incognito Tab**
5. Start browsing privately

Mozilla Firefox

Windows / Mac OS

1. Open **Mozilla Firefox**
2. Click on the 3 horizontal lines in the top right of the window
3. Click on **New Private Window**
4. Start browsing privately

Tip - Keyboard shortcuts to open a new private window: Ctrl-Shift-P (Windows) or Command/cmd-Shift-P (Mac)

Android / iOS

1. Open **Mozilla Firefox**
2. Tap on the **tabs** icon in the top right of the screen
3. Tap on the **mask icon** in the bottom right of the screen
4. Tap on **the plus sign (+)** in the bottom left of the screen to open a new tab
5. Start browsing privately

Safari (MAC and iOS)

MAC OS

1. Open **Safari** from the dock
2. Click on **File** in the top left of the Safari menu bar
3. Select **New Private Window** from the list
4. Start browsing privately

Tip - Keyboard shortcut to open a new private window: Command/cmd-Shift-N

iOS Mobile

1. Open the **Safari** app
2. Tap on **the tabs** icon in the bottom right of the screen
3. Tap on **Private** in the bottom left of the screen
4. Tap on the **plus sign (+)** in the bottom centre of the screen to open a new tab
5. Start browsing privately

An alternative to making these adjustments is to use a privacy extension to your web browser, such as DuckDuckGo. This will ensure that you browse privately all of the time.